Amendments to the Claims:

Please amend claims, as shown. This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-9 (*Cancelled*)

10. (*Previously Presented*) An integrated circuit chip arrangement comprising:

an integrated circuit chip having circuitry therein including a plurality of magnetically-responsive nodes configured to store bits;

a package having magnetic material and covering at least a portion of circuitry in the integrated circuit chip; and

a cryptographic circuit configured to store selected bits of the plurality of magnetically-responsive nodes in an enable register, the value of the bits being responsive to the magnetic material in the package,

wherein the integrated circuit chip is configured to encrypt data as a function of cryptographic key data in the enable register, to mask an output read from the magnetically-responsive nodes using data stored in the enable register and to store the masked output in an output register wherein the package and the plurality of magnetically-responsive nodes are arranged such that removing a portion of the package alters at least one bit of the plurality of magnetically-responsive nodes having a bit stored in the enable register, wherein in response to the at least one bit of the plurality of magnetically-responsive nodes being altered, the data stored in the output register is different than the data stored in the enable register.

11. (*Previously Presented)* The integrated circuit chip arrangement of claim 10 further comprising a sense circuit configured to encrypt data as a function of the selected bits of the plurality of magnetically-responsive nodes.

12. (*Previously Presented*) The integrated circuit chip arrangement of claim 10, wherein the integrated circuit chip is further configured to decrypt data as a function of the selected bits of the plurality of magnetically-responsive nodes.

13. (*Cancelled*)

14. (*Cancelled*)

15. (*Previously Presented*) The integrated circuit chip arrangement of claim 10, wherein the enable register is configured to mask data read from the plurality of magnetically-responsive circuit nodes with data stored in the enable register such that only bits from the magnetically-responsive circuit nodes having a corresponding bit in the enable register are stored in the output register.

16. (*Cancelled*)

17. (*Cancelled*)

18. (*Previously Presented*) A method for protecting data in an integrated circuit chip having magnetically-responsive nodes configured to store data as a function of a magnetic state, the method comprising:

packaging the integrated circuit chip using a packaging material having magnetic material, the magnetic material being arranged to set a magnetic state of a plurality of the magnetically-responsive nodes;

storing an address location of selected ones of the plurality of magnetically-responsive nodes in an enable register; and

using an output from the plurality of magnetically-responsive nodes to decrypt data stored in the integrated circuit chip, wherein using an output from the plurality of magnetically-responsive nodes to decrypt data stored in the integrated circuit chip includes using the address information stored in the enable register to mask an output read from the plurality of magnetically-responsive nodes and storing the masked output in a key register and using the key register to decrypt data.

19. (*Cancelled*)

20. (*Previously Presented*) The method of claim 18, further comprising encrypting data using bits from the selected ones of the plurality of magnetically-responsive nodes having address location information stored in the enable register.

21. (*Previously Presented*) The method of claim 18, wherein storing an address location of selected ones of the plurality of magnetically-responsive nodes in an enable register includes: testing the plurality of magnetically-responsive nodes for stability; and selecting stable ones of the plurality of magnetically-responsive nodes and storing address information for the stable ones of the magnetically-responsive nodes in the enable register.

22. (*Previously Presented*) The method of claim 21, further comprising: testing stable ones of the magnetically-responsive nodes for randomness; and wherein storing address information for the stable ones of the magnetically-responsive nodes in the enable register includes storing address information for selected ones of the magnetically-responsive nodes exhibiting randomness.

23. (*Previously Presented*) The method of claim 22, wherein storing an address location of selected ones of the plurality of magnetically-responsive nodes in an enable register includes storing a data "one" in the enable register for each of the selected ones of the plurality of magnetically-responsive nodes and wherein storing address information for selected ones of the magnetically-responsive nodes exhibiting a selected degree of randomness includes setting a value for selected ones of the magnetically-responsive nodes not exhibiting randomness to a data "zero."

24. (*Original*) The method of claim 18, prior to packaging the integrated circuit chip,

further comprising: selecting a characteristic of magnetic particles in a package to maximize stability of the state of the plurality of magnetically-responsive nodes; and wherein packaging the integrated circuit chip includes arranging the magnetic material in response to the selected characteristic.

25. (*Original*) The method of claim 24, wherein selecting a characteristic of magnetic particles includes selecting at least one of: size and strength characteristics of the magnetic particles.

26. (*Previously Presented*) A method for protecting data in an integrated circuit chip having magnetically-responsive nodes configured to store data as a function of a magnetic state, the method comprising:

packaging the integrated circuit chip using a packaging material having magnetic material, the magnetic material being arranged to set a magnetic state of a plurality of the magnetically-responsive nodes;

storing selected bits of the magnetically-responsive nodes in an enable register; and

masking an output read from the magnetically-responsive nodes using data stored in the enable register and storing masked output in an output register;

wherein the package and the magnetically-responsive nodes are arranged such that removing a portion of the package alters at least one bit of the magnetically-responsive nodes, wherein in response to the at least one bit of the magnetically-responsive nodes being altered, the data stored in the output register is different than the data stored in the enable register.

27. (*Previously Presented*) The method of claim 26, wherein only bits from the magnetically-responsive circuit nodes having a corresponding bit in the enable register are stored in the output register.

28. (*Previously Presented*) The method of claim 26 further comprising encrypting data as a function of the selected bits of the magnetically-responsive nodes.

29. (*Previously Presented*) The method of claim 26 further comprising using data stored the output register for decrypting data stored in the integrated circuit chip.

30. (*Previously Presented*) The method of claim 26, prior to packaging the integrated circuit chip, further comprising: selecting a characteristic of magnetic particles in a package to maximize stability of the state of the plurality of magnetically-responsive nodes; and wherein packaging the integrated circuit chip includes arranging the magnetic material in response to the selected characteristic.